REMARKS/ARGUMENTS

Favorable reconsideration of this application as presently amended and in light of the following remarks is respectfully requested.

Claims 1-3 and 6-26 are currently active, Claims 1, 11, 13, 15, 16, 17 and 18 having been amended, Claims 4 and 5 canceled and new Claims 19-26 added by way of the present amendment.

In the outstanding Official Action Claims 4 and 5 were rejected under 35 USC §112, second para., as having insufficient antecedent basis; Claims 1-9 and 11-18 were rejected under 35 USC §102(e) as being anticipated by Shimizu et al (EP 0982895); and Claim 10 was rejected under 35 USC §103(a) as being obvious over Shimizu et al in view of Leppek (U.S. Patent No. 5,933,501).

In response to the rejection of Claims 4 and 5 under 35 USC §112, second para., Claims 4 and 5 have been cancelled. Thus, this ground for rejection is moot.

In light of the several grounds for rejection on the merits, Claim 1 has been amended to state that –subsequent-- stages receive the sub key output from the round processing circuit of a previous stage and subject the sub key to a round function to output a sub key, and further that --the plurality of round processing circuits comprise at least a pair of round processing circuits having inverse round functions--. Similar changes have been made to the other independent claims. Also, new Claims 19-26 are added to define a varied scope of protection. No new matter has been added, and support for the changes to the claims and the new claims is noted hereinafter.

Before discussing the applied prior art, it is believed that a brief review of the background of the invention and the present invention would be helpful. Applicants' invention relates to a common key encryption system in which decryption is carried out by employing a key (common key or secret key) that is identical to a key employed for

encryption. Various common key encryption systems are known, one of which is a system employing an expanded key, as shown in FIGS. 48 and 49.

For decryption, it is required to employ an expanded key in an order reversed from that for encryption, i.e., in order from expanded key (n) to expanded key (1). However, in a conventional decryption apparatus having an expanded key scheduling section with its configuration similar to that shown in FIG. 48, expanded keys are generated in order from expanded key (1) to expanded key (n). Because of this, for example, prior to processing of the data randomizing section, there has been a need to generate all the expanded keys and store them in a memory.

However, there has been a problem that a device having only poor hardware environment, such as IC card for example, does not have a sufficient storage space for storing all the expanded keys required for decryption.

To overcome this problem, there has been proposed an expanded key scheduling section shown in FIG. 49. An expanded key scheduling process identical to that for encryption is temporarily carried out, and a round function is acted at the last stage, thereby obtaining an output value R_n. Then, the inverse function of each round function is acted with the output value R_n in a stage direction reversed from that for encryption, and expanded keys are generated in order from expanded key (n) to expanded key (1), i.e., in an on-the-fly manner.

However, there has been a problem that a delay time occurs until decryption has been started because of unnecessary time for first generating the same expanded key R_n as that for encryption.

As described above, in the conventional systems, expanded keys cannot be generated in reverse order, thus making it necessary to generate and store all the expanded keys prior to

a decryption process. As a result, there has been insufficient storage space for storing all the expanded keys required for decryption in a poor hardware environment such as IC card, for example.

In contrast to the conventional systems, in Applicants' invention as recited in amended Claim 1, the plurality of round processing circuits (31) comprises at least a pair of round processing circuits (31) having inverse round functions such that the sub key output from the round processing circuit of the last stage being the common key which is input to the round processing circuit of the first stage. Since the inverse functions are used, it is easy to make the sub key output from the round processing circuit of the last stage be the common key.

Therefore, a series of round functions for generating expanded keys is set so as to input a common key and output a value identical to that of the common key, thereby making it possible to generate expanded keys from the common key in the on-the-fly manner in during encryption and during decoding both without consumption of an unnecessary delay time or storage capacity that has occurred conventionally.

New Claims 19 and 23 state that the eight stages are provided and a series of f_1, f_1, f_1, f_1, f_1^{-1}, f_1^{-1}, f_1^{-1}, f_1^{-1} is set to the round functions as described on page 28, lines 18-22.

New Claims 20 and 24 state that the eight stages are provided and a series of f_1, f_2, f_3, f_4, f_4^{-1}, f_3^{-1}, f_2^{-1}, f_1^{-1} is set to the round functions as described on page 27, lines 9-12.

New Claims 21, 22, 25 and 26 state that different sub keys are output from the round circuits even if they have the inverse round functions as shown in FIG. 41. Though the output of a multiplier 240B is used to output a third sub key supplied to 203, the input of the multiplier 242B is not used to output the third sub key. Thus, even if the round functions are inversely determined, the different sub keys are output from the round circuits having the

inverse round functions. Stated differently, even if one of the keys of the round circuits are illegally revealed, the other key is not automatically revealed. This improves the strength of the encryption code.

Turning now to the applied prior art, Shimizu et al. teaches a key transformation section 2 in an encryption processor which is formed of a plurality of key transformation functions fk which are connected in series, as shown in FIG. 2. An encryption key 5 is input to the first key transformation function fk1. A decryption key 6 output from the final key transformation function fkn is used to an input to the first key transformation function fkn in a decryption processor, as shown in FIG. 3.

However, the common key is not input to a round processing circuit of the first stage and a sub key output from a round processing circuit of the last stage is not the same key input to the round processing circuit of the first stage, i.e., the common key. The encryption key 6 is input to the round processing circuit of the first stage and the decryption key 5 is output from the round processing circuit of the last stage.

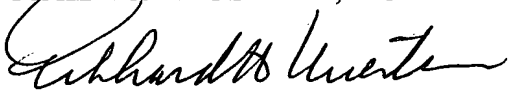
Although the outstanding Official Action states the finding that Shimizu et al. teaches the sub key output from the round processing circuit of a last stage being the common key (FIG. 2, col. 13, lines 27-45), it is respectfully submitted that in fact there is no teaching in Shimizu et al. that the key input to the round processing circuit of the first stage and the sub key output from the round processing circuit of the last stage are common keys. Shimizu et al. merely teaches that the key conversion function fk is constructed of involution functions and thus the common use of circuitry between an encryption conversion and a decryption conversion is allowed (see Shimizu et al., paragraphs [0052] and [0053]). Accordingly, it is respectfully submitted that Shimizu et al. clearly does not anticipate or render obvious the claimed subject matter, and further, that the deficiencies of Shimizu et al. are not remedied by

Leppek. It is therefore respectfully submitted that the outstanding grounds for rejection on the merits have been overcome.

Consequently, in view of the present amendment and in light of the above discussion, no further issues are believed to be outstanding, and the present application is believed to be in condition for formal allowance. An early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

I:\ATTY\EHK\AMEND-RESPONSES\0039\21s\211428US-AMT.DOC